Telefonica

Scope, scale and risk like never before: Securing the Internet of Things_

securely powered by
ElevenPaths

Foreword Telefónica_

Although the Internet of Things (IoT) can be seen as a novelty, it is nothing more than a natural evolution that has finally received a catchy name – a brand that integrates the implications into a single, attractive term. Ever since the Internet first existed, devices have been connected to it. It's just that devices are now smaller, more attractive, better connected and mobile. There are almost infinite advantages on offer from the Internet of Things, but people need to move fast.

It isn't so much that the technology or concept has changed. It's the people that implement, develop, and consume these devices, how they use them and where. The first mention of privacy and security needs to be raised the moment there is mass, normalised consumption. Let's not commit the same mistakes of the past, waiting to the last possible moment to prioritise security and then crying it's too late to modify certain "acquired habits".

Security threats from the IoT are not so different than those in other environments. New security problems have not been created, just evolved from areas such as industrial security, distributed networks and information security. The threats from identity theft are still current today although they now extend to one's own identification between devices.

Denial of Service (DOS) threats are posed from a cloud computing perspective, while malware has been developed – infecting all kinds of systems. The motivations of these threats have not varied too much; rather, they have only intensified and diversified. Attackers will continue to be motivated by economic and ideological reasons, with cyberwar affecting devices present in our lives. As if this isn't enough, attackers see a host of new opportunities in the IoT, with strategic goals to jeopardise the security of critical infrastructures and by definition the security of all citizens.

It's true technology on which the IoT is built has evolved to deal with the scale and diversity of devices (with new names on the scene like Zigbee or 6LoWPan), but we're sure it's just a matter of time

before newly discovered vulnerabilities around these recent technologies will appear. IoT devices have limited resources by definition, but security shouldn't be sacrificed. This is a challenge needing to be solved.

It's therefore vital to act from the first moment, implementing devices where security is of the utmost importance. This is where the IoT will play a fundamental role. It's not just about the privacy of our own data, or the security of our digital identities. In the next few years our lives will be surrounded by devices connected to the Internet that will digitalise every step we take, convert our daily activities into information, distribute any interaction throughout the network and interact with us according to this information. Never before has what we do in our physical lives been closer to the digital world. It is precisely the blurring of the line between the digital world and the real world that represents the changes introduced by the IoT.

Let's understand the problem before it's too late, and guarantee we are able to offer a complete protection plan, taking advantage of all the knowledge that has been developed for other scopes. Gartner puts the Internet of Things right at the Peak of Inflated Expectations on its Hype Cycle for Emerging Technologies[1], suggesting we are some distance from stable and productive behaviours. We all have a lot to do. Because the IoT will be part of our daily lives we can't afford to make the mistakes of the past, where an avalanche of new technology surpasses us. Let's accept the challenge.

Chema Alonso, CEO, Telefónica's ElevenPaths

> Let's understand the problem before it's too late, and guarantee we are able to offer a complete protection plan, taking advantage of all the knowledge developed for other scopes.

Report contents_

Contributor biographies_

Chema Alonso, CEO, Telefónica's ElevenPaths and Telefónica's Global Head of Security

Chema is focused on innovation in security products through proprietary developments and alliances with leading manufacturers and organisations in the industry. He previously ran Informática 64, a computer security and training company, for 14 years. He holds a doctorate in Computer Security from Universidad Rey Juan Carlos in Madrid.

Antonio Guzmán, Scientific Director, Telefónica's ElevenPaths

Antonio has filled more than eight patents related to security, identity and privacy. An author of many articles, he now focuses on privately funded research. In 2005, he co-founded and led a security and privacy investigation group. He also has a PhD in Computer Engineering from Rey Juan Carlos University.

Belisario Contreras, Cyber Security Program Manager, Secretariat of the CICTE

Belisario provides support to the Secretariat of the Inter-American Committee against Terrorism (CICTE) at the Organization of American States. He is involved in cyber security initiatives including the creation and development of Computer Emergency Response Teams (CERTs). He also coordinates outreach and collaboration with other international and regional organisations working on cyber issues.

John Moor, Vice President of Segment Development, NMI

John has more than 30 years of experience in the electronics and microelectronics industries. One of the founders of ClearSpeed Technology in 1997, he joined NMI in 2004, leading development of a number of initiatives including establishing NMI's technical networks and the UK Electronics Skills Foundation. John is also Director of the IoT Security Foundation.

Luis Muñoz, Head of the Network Planning and Mobile Comms Group, University of Cantabria

Professor Muñoz's research focuses on advanced data transmission techniques, heterogeneous wireless multi-hop networks, Internet of Things, smart cities and applied mathematical methods for telecommunications. He has participated in several national and European research projects in which he was, among others, technical manager of SmartSantander.

Andrey Nikishin, Special Project Director, Future Technologies, Kaspersky Lab

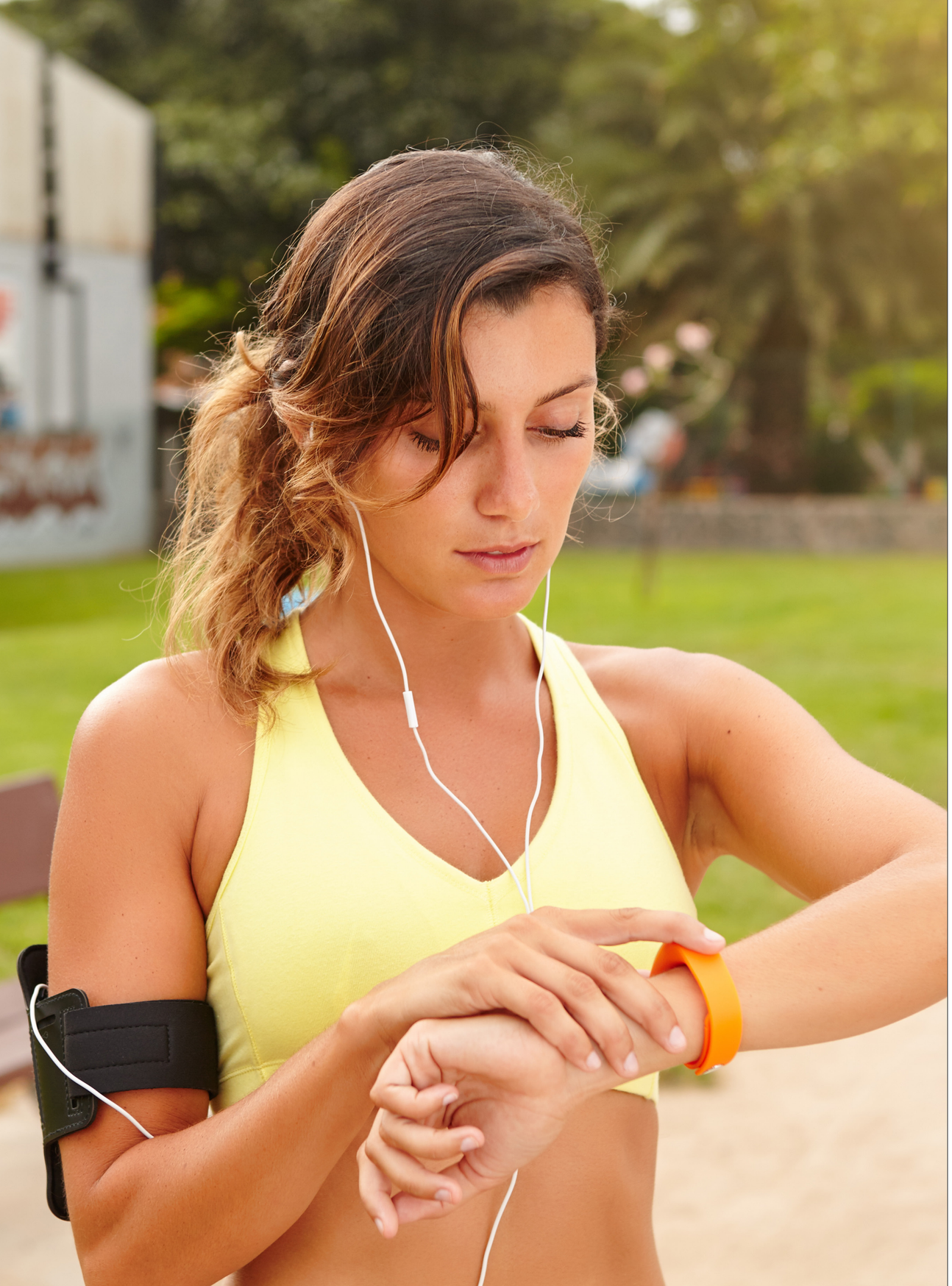
At Kaspersky Lab, Andrey worked as a Senior Software Engineer and Architect before moving to the Strategic Marketing Department as a Product Strategy Manager. Prior to his present role, he headed the Cloud and Content Technologies Research and Development Department. Andrey has experience developing his own antivirus programs.

Bertrand Ramé, Director of Networks and Operators, SIGFOX

Bertrand develops SIGFOX partnerships in Europe and Latin America. He brings 25 years of experience in the telecommunication industry, mainly in business development and general management. He spent half of his career in the US and in the UK, working for companies like AT&T and Telecom Italia.

Jaime Sanz, Telco Technical Account Manager at Intel Corporation Iberia

Jaime provides support for telecommunication accounts in Europe with a main focus on Telefonica for NFV, Datacentre, Security and IoT business. At Intel he worked in different sales and marketing technical support roles, and has a degree in Computer Engineering from the Pontifical University of Salamanca.



Introduction_

The Internet of Things is already unprecedented in terms of scope and scale, changing society and the way people interact with their surroundings, in myriad complex ways. It's entirely fair to say we are nowhere near understanding the ramifications and unintended consequences of what we are doing today – let alone what will be introduced tomorrow and further into the future. Perhaps the most pressing issue is that of security.

"The Internet of Things might be a relatively new term – but the concept is not new. Many of the security issues, bad actors and attacks perpetrated against it are far from new," says Antonio Guzmán of Telefónica's ElevenPaths, "What's different is the scale of the networks involved, the heterogeneity of devices, an incredible reliance on cloud computing and the level of exposure of devices attached to these networks. It is for these reasons that securing the Internet of Things is a real challenge."

"IoT is fast outpacing laws needed to regulate and standardise security measures," says Belisario Contreras, Program Manager for the Inter-American Committee Against Terrorism at the Organization of American States. "This speed of development is also affecting compatibility issues as the security measures for some devices and/or platforms may not be compatible with others as newer versions are released."

And, according to Guzmán, "a lot of the potential problems are merely the same security issues layered on top of infrastructure with a massive scale."

It's creating a business challenge, as well as a technological one.

"There's an increasing realisation that IoT security is a boardroom item and not just an operational cost or technological problem," says John Moor of the IoT Security Foundation. "For big brands especially, there's a lot to lose, and litigation cases are starting to appear in the US where the duty of care organisations have to their customers is coming under scrutiny."

"In my opinion, we are already seeing how Internet of Things is changing our society. As an example, most of the tasks carried out by service providers, users, and others are fully monitored, allowing us to measure the efficiency of

Securing the Internet of Things
Introduction

> There's lots of focus on the innovation opportunities around the IoT – however there has been relatively little on its dark underbelly to date.

the work performed. It's clear that IoT will change our lives even more than the Internet," says Professor Luis Muñoz of the Department of Communications Engineering at the University of Cantabria in Spain, one of the guiding forces behind SmartSantander. "When we started deploying Machine to Machine (M2M) networks in 2000 for managing transport fleets, we were concentrating on a very concrete niche. But now, after 15 years, IoT is present everywhere."

"IoT brings a lot of benefits; as a customer, I'm very pleased to have IoT – it makes life a lot easier," says Andrey Nikishin, Head of Future Technologies Projects at Kaspersky. "But on the other hand, every evolution brings new risks that we haven't thought of. Take the invention of the telephone, for example: at the beginning, no-one considered telephony fraud – nobody really foresaw it. Every new thing carries with it new risks, and new avenues for criminality."

"The same applies to the Internet of Things. The connectivity and interoperability of IoT systems is a boon for, if not criminals, then hooligans. Of course, we can run test scenarios and predict behaviours, but in a connected world you can't do that. People are, by their nature, unpredictable, creative and ingenious. And software's nature is that people make mistakes, and others exploit them."

To John Moor of the IoT Security Foundation, nuance and scale causes complexity, and compounds the challenge.

"In security, limited and small is often a good thing. If you limit the space and the size of the code base, then you reduce the attack surface. When we look at the opportunity of the Internet of Things, we're often looking at massive scale, and hyperconnectivity. From a security viewpoint, it's a daunting proposition," says Moor. "There's lots of focus on the innovation opportunities around IoT – however there has been relatively little on its dark underbelly to date. If we are not careful we could be sleepwalking into a lot of problems – some of which may not have been seen before."

"We need to break the challenges down. People often talk about IoT as if it is one single thing, but in reality there will be many IoT devices out there. Security will be context-dependent and it will be helpful to think of it within that context – for example 'consumer IoT', 'home IoT' or 'healthcare IoT'. That will make a huge difference."

It's a question of focus – security isn't necessarily a priority.

"The Internet of Things is growing exponentially – but not at the pace that could be expected," says Jaime Sanz, Telco Technical Account Manager at Intel Corporation Iberia. "Things like smart cities, connected cars – these add value, but there's also a need to look at how products will create a value chain. There is direction – but at the moment the drive is looking towards connectivity, functionality, power saving and the like – not as much on standards or security."

Telefónica's ElevenPaths' Guzmán sees the problem as one of understanding the demands new territory and opportunity place upon technology.

"In the Internet of Things, barriers are usually defined for industrial environments or critical infrastructure. The type of objects and their number will extend to include all objects or devices of our everyday lives claiming to have computing power," he explains. "In IoT, devices work together to facilitate daily life tasks, making them more efficient and sustainable."

"Depending on the optimised task, you often talk about the so-called Smart Places: Smart Grids, Smart Meters, Smart Homes, Smart Cities, and the like," says Guzmán. "But this collaboration is only possible if the devices are connected to each other and equipped with identification mechanisms uniquely identifying them to all other devices connected to the Internet. This need for interconnection and identification, and even the need to process the information generated or consumed by these objects becomes the problem to be solved when we look at the estimated number of 'things' taking part in the IoT."

This paper will look at three specific areas: the need for universal standards of security, access and control, the clash between Information Technology and an older, more established network of Things – Operational Technology, and the necessities of recovering from breaches, including the impact on users.

Control and access – the real struggle for the Internet of Things_

A much-hyped technological innovation gains pace. Manufacturers, old and new, jump into the market. New ideas spring forth, new markets are created and new standards, if they exist, are shattered.

It's a familiar pattern at the cutting edge of technology, and the Internet of Things is no different from previous waves of innovation. Standardisation is on the back foot – and with it, security.

It's a familiar, probably necessary, cycle that provides impetus, opportunity and innovation at a critical point in time. Arguably, the Internet of Things is at that point: edging towards maturity. It also tends to be the point at which the creation and adoption of security standards, controls and communication is most vital.

Open, or proprietary? Unfettered innovation, or a well-policed set of standards? Especially at periods of rapid innovation, these points of friction become raging conflagrations, before stabilising and entering periods of stable, measured regulation and standards-building.

At the same time, compared to early iterations of large networks – such as telegrams, analogue telephones, cellular phones and the early internet itself – adoption will be chaotic and unplanned.

Such historical projects were often monolithic and thoroughly planned and executed, often by large corporations or government agencies (in the case of telephone networks, often the nationalised postal service of an entire country). Yet, as Gartner Vice President and distinguished analyst Jim Tully[2] observes: "IoT solutions are rarely acquired as a working bundle and simply dropped into an enterprise." The same applies to large implementations built, more often than not, on previously nationalised infrastructure that forms the backbone of the modern Internet."

Looking at the wider picture, large city-wide implementations might fit with the historical model, but it's important to note that individual companies will add their own layers of IoT on top of such installs in the future. And, on a micro level, individuals – and increasingly individual devices and applications – will look to connect to such infrastructure.

The question then becomes: which entity controls what, and how is information passed between networks?

Pace versus control

With the Internet of Things, the application of existing standards, and the creation of new ones, has come up against a hectic pace of innovation. Here businesses need to safeguard their intellectual property as they are making and selling things no-one else can.

The irony is that in order to reap the benefits of IoT devices and services, hardware and software needs to be open and interoperable. Security at the device, application and network layers is vital. But as the pace of adoption increases, so do levels of complexity, variety of implementation and the opportunity for malicious attack or inadvertent error.

Add to this the fact that many IoT manufacturers are relatively new to the software side of the equation[3]. Previous products have focused on hardware value, rather than assessing the total value of hardware when combined with software layers. While the Gartner research applies to licensing and entitlement management for this new class of software vendor, arguably the risk is equally apparent when it comes to creating security from scratch.

Collaboration between connected devices in the Internet of Things requires, by its very nature, openness and mutual trust between devices – and that's built on universal identification and control mechanisms. Openness, combined with precision control, is an absolute must. There needs to be a means to do this across all devices, over and above existing protocols – and there also needs to be a way to gather and manage at scales previously unknown.

"The solution is unlikely to come from contract manufacturers – it's more likely to come from the big brands who have more to lose," says IoTSF's Moor. "If you're a no-name electronics manufacturer, you will be less concerned about loss of reputation or brand than a big vendor with large investments incorporating millions of endpoints. And if you're somewhere in the middle, there's likely to be less reputational risk. Trust needs to be built into the Internet of Things, and the companies that demonstrate resilience to security threats are going to be the ones which are successful."

"Currently there is a speciation of connected products and novelty goods – connected toothbrushes might be an example, for the moment at least. The consumer space is particularly vulnerable, as there are a lot of low cost products on the market with indeterminate origin and manufacture."

It's also vital to remember the roots of the IoT – and the foundations on which much of it is built.

"When we started integrating M2M into transport fleets, that was pioneering work," says Professor Muñoz. "A few years later, European regulation made it compulsory to embed such technology in any truck above a certain weight. The same is happening with our cities. A decade ago, few urban services embedded M2M technology. Now, due to expected population growth as well as the need for improving the quality of life of the citizens, most of the services in the city need to be monitored, aiming at improving efficiency. Citizens want to actively participate in this new era."

For Intel's Sanz, an architectural approach that encompasses both technology and data is a necessary strategy.

"We're involved in every part of the IoT value chain, from the datacentre right down to the chipset in edge devices, barring microcontrollers and sensors. Our belief is that a secure end-to-end architecture is crucial," says Sanz. "Data protection, from edge to cloud as well as at device level, is a must. Thirdly, we're looking at datacentre protection."

"There are two areas when it comes to gateway protection. First is protecting the device before it boots with a combination of Intel SoC Hardware Root of Trust and UEFI Specification. Then there's securing the data with data encryption, integrity protection and whitelisting."

> The consumer space is particularly vulnerable, as there are a lot of low cost products on the market with indeterminate origin and manufacture.

Securing the Internet of Things
Control and access – the real struggle for the Internet of Things

Two worlds collide: IT and OT in the Internet of Things_

Most people are very familiar with Information Technology. But fewer understand – or are even conscious of – the presence of industrial controls. Yet Operational Technology is all-pervasive. It controls the supplies of water, electricity and gas we consume, as well as running the factories that make the things we buy and use.

Today's smart watches are computing marvels, representing many times the processing power of the primitive electronic computers used to land man on the moon. The computer controlling the fuel rods at Chernobyl had capabilities equivalent to a BBC Model B microcomputer, an educational device first introduced in 1981. These two facts are often trotted out – but they singularly miss the point of both the Apollo Guidance Computer[4] and SKALA[5]: you don't need a huge amount of processing power to achieve extraordinary results, especially in very specific applications.

The practice of computerising industrial controls – known as Operational Technology, or OT – predates modern client computing. It is built upon requirements for the controls needed to automate utilities – such as electrical power generation, gas delivery or water – and industry in the most reliable, secure manner possible. Where IT – both in terms of software and hardware – has often been characterised by rapid iteration and innovation at the expense, sometimes, of reliability and other factors, OT is built from the ground up to provide predictable control and measurement.

IT is, by its very nature, designed to be interconnected – while OT is almost exactly the opposite. Yet connecting the two yields significant benefits. It's only in recent years combining IT and OT has become both practical and desirable.

"A combination of the worlds of IT and OT allows us to incorporate real-time data from devices in the field into the business logic of an organisation," notes Telefónica's ElevenPaths' Guzmán. "The combination of IT and OT teaches some very important lessons about how the future Internet of Things can be secured."

"The legacy of OT has meant most IoT deployments have a proprietary protocol using security through obscurity as a defence. The explosion in the number of

devices and verticals is, however, helping fuel a number of initiatives purporting to create open standards for communication – examples include MQTT, Zwave and ZigBee. These are likely to help create more open, usable security standards."

One of the most recent lessons learned is an airgap is no defence. Engineers at Iran's Natanz facility found to their cost that people will, and do, insert USB sticks[6] into PCs controlling operational technology. Suppliers are also attack vectors[7]. Furthermore, interested parties are willing to reverse engineer and design custom attacks to penetrate systems if the value of doing so is significant to them. As the size and scope of IoT networks operated by utilities, cities and large companies grows, the value of such prizes increases accordingly.

Yet OT had decades to develop, giving developers time, scope and budget to carefully plan and approach integration with systems such as ERP (Enterprise Resource Planning), as well as intranet and internet connectivity. The creators of IoT do not have the same timescale over which to consider integration and security. Frankly, their situation is different, coming at a time when many IoT implementations are run over the Internet, open to integration or otherwise prey to possible attack scenarios.

"IT and OT have different philosophies. Biologically, they're not completely different, but the priorities of their creators are. OT engineers want to maintain processes that run 24/7 without interruption. Any interruption of the technological process is a problem, so development is skewed towards the goal of preventing interruption," says Kaspersky's Nikishin. "But for IT engineers, availability of the system is not the main priority. The main problem is to maintain the integrity of data. The main asset in the office network is the data – and again, that skews development."

"When you converge the two, you're going to see a few problems. The IT crowd wants to maintain data security – and that means patching problems as soon as possible. But the application of patches for OT means they have to stop the technological process and contradicts the OT engineer's aims. It's a real challenge to find common ground."

"When you add IoT, it brings a host of benefits and productivity. This process, by the way, is unstoppable and inevitable. The main problem in the Internet of Things is that they are built on the idea of connectivity. As soon as they come into the connected world there are problems."

OT remains a worry for the future – not least because OT implementations are incredibly long-lived.

"The security of data as well as reliability of operation are important," says Nikishin. "It goes almost without saying, but IoT has influence on our day to day lives. The main goal for the IoT is to design all of the devices with security in mind from the very beginning. Otherwise, they are almost impossible to secure."

Securing the Internet of Things
Two worlds collide: IT and OT in the Internet of Things

> "The main goal for the IoT is to design devices with security in mind from the very beginning.

"This device should be designed from the very beginning to be secure. Our idea is to force all manufacturers of industrial devices – SCADA, PLCs and PLMs – to redesign all of their systems as secure, and to force customers to upgrade their existing control structure to a new one. A system should be secure by design. When you look at what Siemens did after Stuxnet, you'll see what I mean. They did a large amount of work, to hugely improve the security of their OT. But getting customers to change their systems – which might have been running perfectly on the same PLCs and PLMs for 10 or 15 years, proved more problematic. Simply put: the users saw the cost, believed their systems weren't broken, and refused to fix them."

For OAS' Contreras, the advent of IoT and increasing interconnection of IT and OT environments helped jumpstart change within the OT industry – and also placed new responsibilities on the heads of technical personnel.

"Not so long ago, the air gap was considered security enough for OT. The growth of IoT blurs the lines considerably and OTs are now being brought into the world of IT with increased connectivity and threat vectors. Engineers and other technical personnel will be expected to handle both IT and OT needs, and the same will be true for cybersecurity technicians," says Contreras. "IoT's role as a collector, distributor and receiver of data will make IT and OT more responsive to problems or environmental changes and allow them to operate more flexibly and efficiently. It will also require CIOs to explore information flow and question how company data is stored. This will also act as a business opportunity as with this correlation of data many businesses can now project business growth on better information."

"We also need to consider society's requirements and constraints. At the beginning, IoT technology was pushed by companies, research centres and the like, which saw a unique opportunity. It took a little more time for the citizens to see the benefits that such technology might bring them and hence move from a reluctant position to an enthusiastic one. As I already said, IoT is implicitly stimulating a behavioural change," says Professor Muñoz.

"People in Santander are getting more and more skilled in using and interpreting the information IoT and supported services provide them. This is clear evidence we are overcoming one of the threats always invoked, namely, the digital gap. In this sense, I would say that more than the technological challenge we faced when we started the SmartSantander project, we were facing a new way to manage and live in the city. In short, we were reshaping the city ecosystem driving towards a new paradigm based on the knowledge of and the intensive use of ICT."

Securing the Internet of Things – before and after_

The networks IoT creates will be some of the biggest the world has ever seen, making them enormously valuable to attackers.

By the measure of Metcalfe's Law[8], the value of IoT networks is massive, making them significant targets for attackers motivated by greed or political cause. Yet, if IoT represents a difficult security task now, as the number of networks, operators, consumers and devices spirals, so does the risk of a successful breach.

Part of the problem is scale; the sheer number of devices, networks, applications, platforms and actors creates a Wicked Problem[9] that will only grow in complexity as the infrastructure to support, serve and extract value from the IoT grows.

The intentions of designers – who prioritise safety over security, as we have seen earlier – may also create a problem.

"We have to sacrifice the heterogeneity of devices for the ability to control and secure them," says Telefónica's ElevenPaths' Guzmán. "The security layer of IoT must contemplate protection systems at all levels – network layer, application layer and IT devices."

Managing vulnerabilities and responding to attacks or breaches is something that's possible now because of the relatively limited number and scope of IoT devices. Getting the security, reporting and resolution processes in place for internet connected devices before the first catastrophic attack will be absolutely vital.

Recent proofs of concept, such as the breach of Chrysler's[10] security on 1.4 million Jeeps that could be updated over the air and remotely controlled by a malicious attacker, demonstrates the potential problems around connecting IoT devices to networks.

It's also worth considering an attack may not be necessary to force change. An accident, inadvertent slip or honest mistake could also be catastrophic – we can go back as far as the 1988 Morris Worm[11] for an example. While scale and variety could well help prevent significant damage, it's still the case that the pace of development, scale and growth of IoT enables far more potentially damaging outcomes than seen before in more traditional computing environments.

"Balancing the creativity of invention against the need to secure is tough – but also necessary," says Guzmán. "And

It's important to understand that with great connectivity, comes great responsibility.

while, at first glance, it may appear to stifle innovation, the opposite is the case. I mentioned security by design, and it's not necessarily something that stifles innovation," says Kaspersky's Nikishin.

"Also, innovation brings lots of new companies into the market, but it's unfair to single new entrants out as being any more risky than others. A lot of existing manufacturers try to adapt existing designs with unexpected consequences. For example, there are lots of benefits to consumers from having utility smart meters. But in Spain in particular, the introduction of these meters has brought several problems to the surface. Users can hack them to underreport consumption – and that's lost revenue. Some meters were using 3G to transmit readings, and people found a way to use it to get free Internet access. We're talking about a country here with between 30 and 40 million installed smart meters."

"The thing is that this isn't negligence; it's the unintended consequences I talked about earlier, coupled with a fundamental change to the approach manufacturers need to take. This sort of company designs for safety – and there's no certification or security standard for IoT devices to refer to. This is a problem with established manufacturers and engineers who think primarily about safety rather than security."

"Then there are new companies. One business we have helped makes smart home devices – motion detectors, electricity monitors, temperature monitors, sensors of all kinds. They store and process a lot of the data in the cloud – and decisions based on that data are made there, too. This allowed the company to build some very smart systems that adapt to a household's requirements, and develop new services and products very quickly."

"None of this data was encrypted. While someone switching a light on or off might not seem that important, anyone wanting to break into your home would probably be really interested in the pattern of household occupancy. Also, because the decisions are made in the cloud, what happens if there's not 100% connectivity in all these home devices?"

IoTSF's Moor sees a three-pronged approach as being the most successful.

"We have to think security first – and secure by default," said Moor "You can't bolt on security after the event. Yet some companies are having to try and do that as they've rushed to market. They are motivated by the market opportunity of bolting in connectivity without understanding the wider implications. It's important to understand that with great connectivity, comes great responsibility."

"You may not create a problem for yourself, but you may create one for others elsewhere, and the more problems the market encounters, the slower the adoption rates will be as risk and uncertainty dominate. When someone can break into your home network through your connected kettle (and incidentally, they might be able to), you start seeing what people have on their home networks that could be of interest to rogues of all denominations."

"Secondly," says Moor, "We've got to develop for resilience. No-one makes an unbreakable product, but the chances of getting hacked increase as a product becomes more successful and ubiquitous. Companies need to think about how to respond to attacks when their products are in active use. And they need to be secure at scale from cradle to grave. Right from manufacture, the assets you think you have are validated and authenticated. Even in the chip space, Texas Instruments and IBM are teaming up to create unique identifiers in chips to follow them in their life cycle. Where IoT is being applied, they're not necessarily in throwaway devices. Some can live for decades. When you think of things like software updates, there are a lot of challenges. When I think of the number of connected devices just in my home, the idea of them all updating all the time – well, it's going to create havoc. Then there'll be the second hand market."

"Finally, there's fitness for purpose. Security in IoT doesn't have a universal solution. We're talking about context here – the application will determine a number of factors which will mandate the approach companies adopt to securing their systems. For example, the economics of deploying millions of devices will dictate the cost of manufacture, the provisioning of systems, the maintenance of security regimes etc, and the criticality of those systems will determine the level of security needed – for example consider a medical implant and the threat of hacking as opposed to a lightbulb."

Antonio Guzmán of Telefónica's ElevenPaths sees the problem in terms of old challenges to new infrastructure and massive scale:

"Traditional approaches must be reconsidered," says Guzmán. "Schemas where prevention, detection and response strategies live together allow solutions that continuously monitor both the interior and outside of infrastructure to prevent attack, alert if an attack is happening and, should one be successful, perform a recovery and a response."

"But for IoT, the scale makes current solutions ineffective and inefficient. We need to propose a new way of securing what is a new wave of technology that can work at the scale we – and everyone else – anticipates. We need to cover four key OSI layers; transport, physical and infrastructure, the application, device and field network layers. I mention OSI because these layers are not new – they're part of the original makeup of Ethernet networks – but the challenges they present as part of the Internet of Things are magnitudes greater than what we've had to deal with as a society before."

Conclusion_

The networks IoT creates will be some of the biggest the world has ever seen. And that makes them enormously valuable to attackers.

Long before the Internet of Things became common parlance, it was apparent that the world would run out of possible addresses for internet-connected devices available through IP v4 (4,294,967,296, to be exact).

While the Internet of Things will not expand to consume all of the 3.4*1038 available for the foreseeable future, it is apparent that it is already growing far faster – and with a far higher knowledgeable user base – than its next largest predecessor – the Internet itself. This raises significant concern. People, devices, applications, networks and physical infrastructure must be protected – and the best way to do this is to work to and build upon common standards.

"Every single new technology comes with hurdles and expectations – and sometimes, big threats," says Bertrand Ramé, Director of Networks and Operations at SIGFOX. "At SIGFOX, we consider both the integrity of the device as well as the privacy of the user data, especially when we're going to connect almost every single physical thing to the Internet. Besides, IoT applications may need to implement different levels of security to match the business criticality, budget and power consumption, above that mandated by governments, manufacturers, and institutions."

"We're really early on with the Internet of Things," says Moor. "I think we'll know we have made it when it becomes invisible, and people stop talking about IoT and focus more on experiences and new, valuable and as yet undiscovered services. When it's this pervasive, and "the Internet and the thing" has passed out of the public consciousness, when physical objects you rent or buy just set themselves up and

> The Internet of Things will allow for individuals, companies and states to have more control over their technology, as well as greater access to information, than ever before.

maintain themselves, that's when we've made it. To get there, today's Internet of Things needs to be trusted in the wild and fundamentally secured."

"The Internet of ThIngs will allow for individuals, companies and states to have more control over their technology, as well as greater access to information, than ever before. The major security problem associated with IoT is the widespread risk that one vulnerability could bring down an entire system. This shouldn't deter us, however, from taking advantage of these innovations," says OAS' Contreras.

"As we implement IoTs into our network we will want to ask the following questions: 'Will the potential benefits of IoT outweigh the potential risks in this particular circumstance?', 'Is my network protected with updated security measures, and does the IoT developer have a good track record for security?' and 'Do I know how and where the data being collected is stored, and is the storage location secure and protected by measures such as passwords and encryption?'. If we consider these concerns, we can welcome IoT innovation while maintaining our ability to respond quickly if our cybersecurity is threatened."

"In order to reap the benefit of the IoT securely, we will need a three-pronged approach to security. Firstly, standards and regulations for IoT software development and deployment have to be established. There needs to be trust and consistent dialogue between developers and operators; and finally, there has to be a more holistic understanding of cybersecurity, taking into account IoT and the way it connects IT and OT systems."

Standardisation efforts are underway – and are proving successful. However, a way to ensure the multiplicity of actors can interoperate and communicate security requirements, needs and risks at scales dwarfing current problems is vital. It's not necessarily something we have – or will have soon. We need to work towards it, however. In fact, we must.

Appendix_

1,2 Gartner – Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor
http://www.gartner.com/newsroom/id/3114217

3 Gartner – Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor
http://www.gartner.com/document/3143217

4 Computer Weekly – Apollo 11: The computers that put man on the moon
http://www.computerweekly.com/feature/Apollo-11-The-computers-that-put-man-on-the-moon

5 Chernobyl Nuclear Power Plant: Control Room
http://kiev2010.com/2010/06/chernobyl-nuclear-power-plant-i-control-room

6 IEEE Spectrum: The real story of Stuxnet
http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

7 Engadget – Stuxnet worm entered Iran's nuclear facilities through hacked suppliers
http://www.engadget.com/2014/11/13/stuxnet-worm-targeted-companies-first

8 P2P Foundation – Metcalfe's Law
http://p2pfoundation.net/Metcalfe's_Law

9 Rittel, Webber – Dilemmas in a General Theory of Planning
http://www.uctc.net/mwebber/Rittel+Webber+Dilemmas+General_Theory_of_Planning.pdf

10 Wired – Hackers Remotely Kill a Jeep on the Highway—With Me in It
http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

11 ZDNet – The Morris Worm: Internet malware turns 25 | ZDNet
www.zdnet.com/article/the-morris-worm-internet-malware-turns-25

Telefonica

securely powered by

ElevenPaths

For more information about ElevenPaths,
visit elevenpaths.com or follow on
Twitter at @elevenpaths and LinkedIn.